Microsoft

.net developer training

Create XML Web Services and Applications with Visual Studio .NET

Security in .NET

Module 11 Agenda

- Security in .NET
  - Introduction
  - Authentication
  - Authorization
  - Summary

Introduction
Security in .NET

- Types of Security in .NET
  - Authentication and Authorization
  - Evidence-based Security
    - Policy model for granting permissions
  - Code Access Security
    - Control what code can do
- Application Security features have been added to .NET
  - Reduces time developers need to create security features
  - Provides standard security system
    - Different approaches for different problems

Authentication And Authorization

- Authentication
  - Web Applications authentication
  - IIS authentication
  - Forms-based Authentication
  - Windows® Application authentication
- Authorization strategies
  - Role-based Security
  - Web Application authorization
  - Configuring user and role authorization

.NET Security
Core Concepts: Authentication

- Process of verifying identity by comparing credentials against an authority
- Non-authentication = Anonymous user
- Basic, Digest, Passport, NTLM, Kerberos and custom or application specific security

Web Application Authentication Topics

- Types of authentication
  - Windows, integrating with Internet Information Server 5.0
  - Passport, centralized services provided by Microsoft
  - Cookie/Forms-based

Internet Information Server Authentication

- ASP.NET applications sit atop IIS
  - Takes advantage of IIS and Windows Security
- Internet Information Server basics
  - Set in Internet Service Manager
- Impersonation
  - IIS authenticates the user (before the request is passed to ASP.NET)
  - A token is passed to ASP.NET application
  - ASP.NET does not impersonate the token by default
  - Access is permitted according to NTFS

Forms-based Authentication

- User visits URL in protected site
  - User is redirected to login page
  - User enters username and password
    - ASP.NET matches these with server credentials
      - Code on server authenticates user
    - Browser is redirected to requested page
      - Server sends cookie to browser
    - Authentication cookie is provided automatically on subsequent pages

Windows Application Authentication

- Types of authentication
  - Windows - NTLM or Kerberos
  - Passport, centralized services provided by Microsoft
  - Forms-based (similar to Web Applications)

.NET Security
Core Concepts: Authorization

- Authorization occurs after authentication
- Uses a principal's identity to determine access rights to resources

Authorization Strategies

- All .NET applications
  - Role-based (explicit) Authorization
  - Custom authorization
  - Windows Security and ACLs
  - Declarative method authorization
- ASP.NET
  - URL authorization

Authorization Strategies
Role-based Security

- Allows logic execution based on requestor's identity and/or roles
- Support for…
  - NT accounts/groups
  - Custom defined users/roles sources
  - Managed COM+ 1.0 Services for Windows account-based roles

Authorization Strategies
Accessing Role-based Security

- Use the identity and principal objects
  - Authorization code is the same for Web and Windows Applications
  - Custom authentication and authorization
    - GenericIdentity and GenericPrincipal
  - Windows authentication and authorization
    - WindowsIdentity and WindowsPrincipal

Authorization Strategies
Demo

- Windows Application Authorization

Custom Web Authorization

- Handle AuthorizeRequest event
  - Application level (global.asax)
  - Http module (implement IHttpModule)
- Scenarios:
  - Implement per-request billing system
  - Restrict access based on the time of day or other custom parameters
  - Restrict access based on dynamic behaviors (e.g., implement a per-day access limit)

Declarative Authorization

- Implement with custom attributes
- Part of a method's metadata
- JIT converts annotation to a check

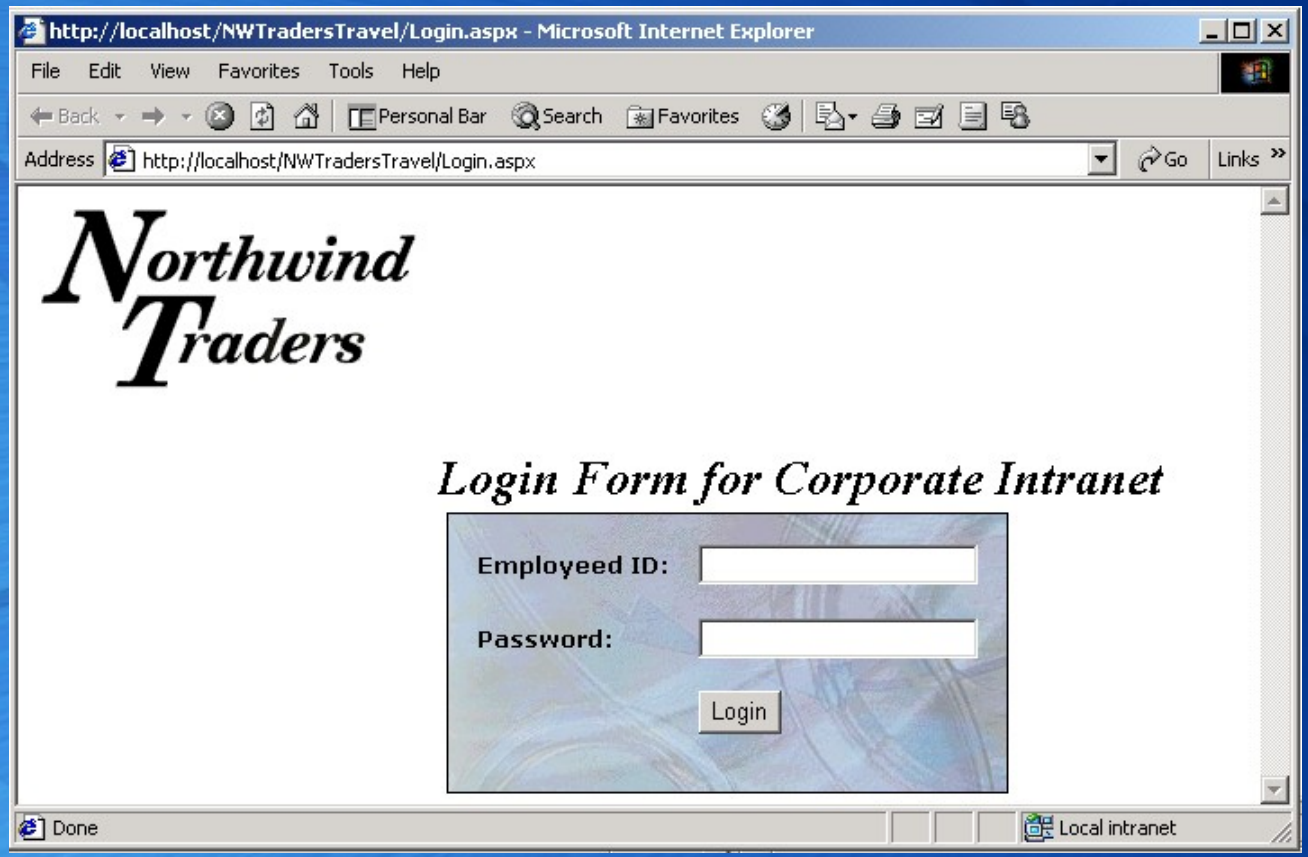
Web Application Authorization
Configuring User And Role Authorization

- Configure in Web.Config

```
< authorization>
        <Allow
            user= "Ken"
            roles= " MyCo\
  Engineers"/>
        <deny users= "*"/>
  </authorization>
```

Web Application Authorization
Demo

- **Web Application Authorization**



Summary

- Authentication
- Authorization

Resources

- ***Microsoft .NET Framework Security Overview:***

  http://msdn.microsoft.com/vstudio/nextgen/technology/frameworksec.asp

Microsoft®

11.22